



## An Analysis of Cybercrime Awareness Amongst First Year Students in Nigerian Private University

Balogun O\*, Hinmikaiye J, Adegbenle A.A, Oyebode A.A, Akinshola J, Nzenwata U.J

Department of Computer Science, Babcock University, Nigeria

### ABSTRACT

The prevalence of Cybercrime the World over threatens to destroy the very fabric of peace. From financial fraud to theft identity, the ways in which this act continue to evolve and penetrate the most secure of digital entities calls for worry.

A more disturbing trend is the perception of Nigerians being the purveyor of such acts. This study therefore seeks to find out what young Nigerians actually know about cybercrimes in order to gain an insight into what actually drives it and if possible, to discourage such acts from a tender age.

Results show the perception of the World is not unfounded and recommendations that may go a long way in making this venture unattractive is highlighted.

**Keywords:** Cybercrime Awareness, First Year Students, Nigerian Private University

### \*Correspondence to Author:

Balogun O

Department of Computer Science,  
Babcock University, Nigeria

### How to cite this article:

Balogun O, Hinmikaiye J, Adegbenle A.A, Oyebode A.A, Akinshola J, Nzenwata U.J. An Analysis of Cybercrime Awareness Amongst First Year Students in Nigerian Private University. Research Journal of Mathematics and Computer Science, 2019; 3:15



eSciPub LLC, Houston, TX USA.

Website: <https://escipub.com/>

## Introduction

The English Oxford living dictionaries (2019) defines crime as an action or omission which constitutes an offence and is punishable by law. It also defines internet technology related crime, otherwise known as Cybercrime as criminal activities carried out by means of computers or the Internet.

Cybercrime represents an extension of the conventional criminal behavior alongside some novel illegal activities. This phenomenon is one of the most serious social problems in our society today. It has threatened the credibility and sabotaged the external image of Nigeria which invariably has a greater effect on the society at large (Abdul-Rasheed, Lateef, & Yinusa, 2016)

With a median age of 17.9 from an estimated 200 million people (worldometers, 2017) in Nigeria, cybercrimes are performed by people of all ages but with a dominant number in the youth age group. They go into it for the purpose of profit making, getting busy, and social standings.

The conscious and continued effort to decrease the prices of digital gadgets, making them readily available, and the continued development of internet-based applications that speed up our of formal and informal interactions' processes have also given room for the explosion of cybercrimes. This activity has become so tuned-into that many people no longer see it as a crime and current trends in Nigeria show that some have resorted to it as a career.

A report on cybercrimes by Deloitte titled '2018 Nigeria cybersecurity outlook' (Deloitte, 2018) shows that the tide of cybercrimes in Nigeria is getting stronger and have taking various forms. The report posits that ransomware won't fade out anytime soon, cyber-criminals are increasingly turning to crypto-currency, and there is an increase in cloud based attacks. For organizations to safe-guard against theft of all forms, keep the report posits that cyber security regulations have to keep evolving and organizations have to battle for the best hands

to combat it (in most cases, paying top-dollar to recruit the best).

The effect of cybercrime ranges between psychological and physical. In some cases, it has been known to cause the death of victims. Cybercrimes are also known to have an attendant effect on other social vices like drugs production and abuse, human trafficking, and terrorism which globally generated an illicit profit of \$1.5 trillion in 2018 (Ismail, 2018) and is projected to have a global economic effect of \$6 trillion by the year 2021.

This work therefore seeks to analyze the level of cybercrimes awareness with a focus on new intakes (undergraduates) into the Nigeria University system.

The aim of this research is to understand the level of awareness of cybercrimes among 100 level students in the Nigeria university system and to ascertain what drives it.

The scope of study involves gathering data from students in 100 level i.e. the first year students from a private university located in Ota, Ogun state, Nigeria.

Various texts have showed the relationship between Cyber-crimes and other social vices. This makes it important to understand the mindset of the younger generation i.e. young adults who will have to contend with the issues that cybercrimes may pose in the future.

## Literature Review

Gordon Moore, a co-founder of Intel, in 1960, identified the trend of continued fall in prices of information technology related gadgets. This trend which was coined into what is today known as Moore's law states that

"Every year or two, the capacity of computers double inexpensively" (Java How To Program, 2015, p. 4)

The trend of getting high capacity gadgets for low prices has affected the way we carry out our daily transactions. It has made us humans more technologically savvy but has also unfortunately brought about an astronomical spike in technology related criminality.

Solaka D and Topaloglu M (2015) analysed the perception of Cyber Crimes in the view of Computer Science Students at Trakya University in terms of demographic factors. Their collected data via questionnaires showed that there is more need for sensitization because people had a blurry understanding of what theft constitutes and what it isn't. But, they tainted their data when they administered questionnaires to people outside the scope of their study which may have had a significant impact on the result obtained.

Michael Levi (2016) assessed the trends, scale and nature of economic cybercrimes. The work realized that taking a holistic view of cybercrimes, there were little differences on the modulus operandi and causative factors that allow it to open. Given the indices that cybercrimes are measured against in Canada, US, Switzerland, Australia, and China, the work didn't show a clear telemetry of whether Cyber criminality is winning or measured put in place to fight against it and what metrics will be broadly acceptable for measurements.

Bhavna Arora (2016) explored and analyzed Internet crimes and their behaviors. This work identified the various type of cybercrimes schemes and trends so as to mitigate against cyber-attacks. Their work showed that lack of awareness in the first place was the bane against the fight against it. Although this work was able to identify the various schemes of cybercrimes, it failed to address the patterns and dynamism of cybercrimes. As trends continue to unfold, it didn't show how these technologies are developed, who and what organizations to look to in the event that something new happens.

Mohammad Rasmi and Aman Jantan (2016) looked into the Social and contextual taxonomy of cybercrime with respect to Socioeconomic theory of Nigerian cybercriminals. The work was able to establish the causative factors and effect peculiarities of cybercrimes in Nigeria while placing them in various categories with reference to what the realities (socioeconomic, psychosocial and geopolitical) are at different

times of the economic life-cycle of Nigeria. The work failed to show the deep-rooted lines of deliberate inefficiencies and sabotage that makes prosecuting and fighting cybercrimes and all other types of graft, a herculean task in the Nigeria. #

Haruna et al (2015) did a review of the advances in Cyber Security Benchmark Datasets for Evaluating Data-Driven based Intrusion Detection Systems. They realized that Knowledge discovery in databases where no longer reliable for state-of-the-art cyber security benchmark datasets. The Australia defence force academy Linux based intrusion system was not well explained and didn't show how it will incorporate currently popular datasets.

## METHODOLOGY

Our data collection method was through questionnaires. The questions made use of open-ended and close-ended answers. Some questions were decoy in nature to give a pointer to the level of sincerity of the answers given by respondents. Our closed ended questions made use of the 6 point Likert scale.

To emphasize the need for un-manipulated data, the survey questions were not gender related and was distributed by peers of the group.

To ensure that results were a true reflection of the state of things, we made use of simple random sampling for our respondents. Also making use of judgmental sampling technique, a total of 51 out of questionnaires were used for the result analysis.

## Result Analysis

The following are results obtained from the questionnaires distributed, retrieved and used for the purpose of this study

- i. On the question of if respondents are aware of the existence of Cybercrimes, 100% affirmed that it does exist.
- ii. On the question of if they truly understand what cybercrimes entails, 51% strongly agreed.

- iii. On the question of if they have indulged in any form of cybercrime, 89% answered No
- iv. On the question of if they have been involved in activities like unauthorized downloads of contents (e.g. movies and books) and unauthorized use of Wi-Fi, 68% answered Yes
- v. On the question of if they know that partaking in any of such activities in (iv) is also a form of cybercrime, 74% strongly agreed.
- vi. On the question of if they are familiar with someone who is into cyber-criminality, 51% answered Yes
- vii. On the question of if they are willing to disassociate themselves from such a person in (vi), 19% answered Yes.
- viii. On the question of the type of relationship between the person in (vi) and respondent, 60% said they are friends, 40% reported that they don't particularly have any form of relationship with that person, while 0% was reported for a family member
- ix. On the question of if they indulge in other social vices like gambling, alcohol consumption, smoking, etc. 24% answered Yes
- x. On the question of what they thought was the most influencing factor for participating in cybercrimes amongst their age and academic class bracket, 66% answered that it was mere greed, 25% alluded it to peer pressure, while 9% alluded it to gaining as much to impress the opposite sex.
- xi. On the question of if they were aware of the bad perception the rest of the world has for Nigeria as a result of cybercrimes was not unfounded, 82% strongly agreed.

Data obtained show as disturbing pattern. At first we see that respondents are aware of the menace of cybercrimes but are delusional of their participation in one form or the other. The result also shows that a sizeable amount of them

are not willing disassociate themselves with friends who are into cybercrime. This means that in the long run, a number of them who are not into cybercrimes may become initiated to it in the nearest future.

Data shows that somehow, respondents feel that even though they know it is wrong, they think that there is a big difference between those who involve themselves with financially related cybercrime and those who just download books or movies.

Our results also collaborates the position of Ismail (2018) about the relationship between cybercrimes and other social vices which our result shows to be 24%. Given that the average age of 100 level students is 16 years in Nigeria, and with our result also showing a 25% allusion for involvement in cybercrime as peer-pressure and just 19% willing to sever the ties of such friendships, it is safe to say that the number of youth involved in this immoral activity may increase.

On a more encouraging note, data shows that respondents understand how they are perceived as Nigerians and agree that the perception is not misplaced.

### Conclusion and Recommendation

This study looked into ascertaining the level of cybercrime awareness among fresh undergraduates. Our results show a lot has to be done by all and sundry if we are to stem the tide of cybercrimes amongst Nigerian youths.

It is therefore recommended that sensitization programs about the devastating impact of cybercrimes on the society and the world at large should be formulated and tailored towards setting the Nigerian youth on a moral path

### References

1. English Oxford Living Dictionaries. (2019, March 8). *Crime*. Retrieved from Lexico: <https://en.oxforddictionaries.com/definition/crime>
2. Ismail, N. (2018, April 24). *Global cybercrime economy generates over \$1.5TN, according to new study*. Retrieved from Information Age: <https://www.information-age.com/global->

cybercrime-economy-generates-over-1-5tn-according-to-new-study-123471631/

3. I., A. A., Haruna, C., Muazc, S. A., & Ila, L. B. (2015). A Review of the Advances in Cyber Security Benchmark Datasets for evaluating Data-Driven based Intrusion Detection Systems .*Procedia Computer Science*, 62, 221-227. doi:10.1016/j.procs.2015.08.443
4. Solaka, D., & Topaloglua, M. (2015). The Perception Analysis of Cyber Crimes In View of Computer. *Procedia - Social and Behavioral Sciences*, 182, 590 – 595. doi:10.1016/j.sbspro.2015.04.787
5. Abdul-Rasheed, S. L., Lateef, I., & Yinusa, M. A. (2016, August). Cybercrime and Nigeria's External Image:. *Africology: The Journal of Pan African Studies*, 9(6), 119-132. Retrieved from file:///C:/Users/lenovo/Downloads/CYBERCRIME ANDNIGERIAEXTERNALIMAGE.pdf
6. Deitel, P. D. (2015). *Java™ How to Program* (10th ed.). Boston: Pearson. Retrieved June 12, 2019
7. worldometers. (2017). Nigeria Population (LIVE). Retrieved March 9, 2019, from <http://www.worldometers.info/world-population/nigeria-population/>
8. Levi, M. (2016, October 11). Assessing the trends, scale and nature of economic cybercrimes: overview and Issues. *Crime, Law and Social Change*, 67(1), 3-20. doi:10.1007/s10611-016-9645-3
9. Rasmi, M., & Jantan, A. (2013). A New Algorithm to Estimate the Similarity between the Intentions. *Procedia Technology*, 11(47), 540 – 547. doi: 10.1016/j.protcy.2013.12.226

